



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/855,908	05/15/2001	Steven Michael Bellovin	2000-0284	1152

42292 7590 08/11/2004

LAW OFFICE OF JEFFREY M. WEINICK, LLC
615 WEST MT. PLEASANT AVENUE
LIVINGSTON, NJ 07039

EXAMINER

HAYES, JOHN W

ART UNIT PAPER NUMBER

3621

DATE MAILED: 08/11/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/855,908

Applicant(s)

BELLOVIN ET AL.

Examiner

John W Hayes

Art Unit

3621

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 07 May 2004.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-11 and 17-21 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-11 and 17-21 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☒ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 15 May 2001 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Status of Claims

1. Applicant has amended claims 1-9 and 11, added new claims 18-21 and canceled claims 12-16 in the amendment filed 7 May 2004. Thus, claims 1-11 and 17-21 remain pending and are presented for examination.

Response to Arguments

2. Applicants argument filed 7 May 2004 have been fully considered but are either not persuasive or moot based on the new grounds of rejection.

3. Applicant argues that Franklin discloses a customer ID account number that is obtained by registration and that this customer ID account number is not hidden from the merchant or safeguarded against online eavesdropping. Examiner submits that the customer ID number taught by Franklin is only used to identify the customer rather than an account number. Franklin discloses that the issuing institution only uses the customer ID number to identify the customer and to look up the real customer account number which is hidden from the merchant and any other persons who may be eavesdropping.

4. Applicant further argues that Franklin teaches using only a four digit portion of the transaction number that contains a MAC that is specific to the online transaction with the merchant while the present invention provides a verification by a comparison of "multiple fields or encrypted information" with corresponding transaction information provided by the merchant. Examiner submits that Franklin teaches a similar method of using multiple fields of information such as cardholder data, transaction amount, merchant ID, goods ID, time and transaction date to calculate a MAC as a function of the user's private key which would inherently result in encrypted information. Franklin specifically discloses that the unique MAC is generated through the use of a cryptographic hashing function (Col. 5, lines 32-36). Franklin, however, discloses that the issuing institution uses the same cryptographic hashing function to compute a MAC and then compares the generated MAC with the MAC provided by the merchant. The present invention differs since

Art Unit: 3621

it recites matching decoded fields of information with corresponding transaction information rather than comparing MACs. Examiner, however, has provided a secondary reference to Walker that more clearly discloses this feature.

Specification

5. The disclosure is objected to because it contains an embedded hyperlink and/or other form of browser-executable code (See page 2, paragraph 0003). Applicant is required to delete the embedded hyperlink and/or other form of browser-executable code. See MPEP § 608.01. Appropriate correction is required.

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

7. Claims 1-11 and 17-21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Franklin et al, U.S. Patent No. 6,000,832 in view of Walker et al, U.S. Patent No. 6,163,771.

As per **Claims 1 and 11**, Franklin et al disclose a method for facilitating credit card transactions over a telecommunications network without disclosing a credit card account number, comprising the steps of:

- receiving from a merchant, via the telecommunications network an encoded temporary transaction authorization number for an e-commerce transaction, said temporary transaction number having been generated by a user having an account with a credit card issuer, wherein said temporary transaction authorization number comprises multiple fields of encrypted

Art Unit: 3621

information regarding the transaction such as a MAC (Abstract; Col. 2, lines 8-21; Col. 5, lines 25-57);

- retrieving secret information required to generate a similar MAC (Col. 5 line 65-Col. 6 line 5; Col. 12, lines 10-15); and

- matching the generated MAC with corresponding information provided by the merchant, and thereby verifying the temporary authorization transaction without disclosing the credit card account number via the telecommunications network to the merchant (Col. 6, lines 1-12; Col. 12, lines 15-25).

Franklin discloses that the issuing institution uses the same cryptographic hashing function to compute a MAC and then compares the generated MAC with the MAC provided by the merchant, however, fails to disclose matching decoded fields of information with corresponding transaction information as recited in the claims. Walker et al disclose a method for generating a single-use financial account number by encrypting multiple fields of information such as a an initialization variable, an a-bit account number and a nonce (Col. 7, lines 60-67; Col. 8, lines 8-36). Walker further discloses looking up secret information such as the cardholder's private key to decrypt the fields of information and compares this information to validate the transaction (Col. 8, lines 40-67). Walker et al further disclose that instead of encoding the account number as part of the credit card number, the name that appears on the card could take the place of the account number and further that more bits become available and can be used to encode a timestamp, purchase information or even merchant information (Col. 11, lines 8-19). Thus, it would have been obvious to one having ordinary skill in the art at the time of applicant's invention to modify the invention of Franklin and encrypt multiple fields of information by the user and then decrypt this information by the issuing institution and perform a comparison to validate the transaction as taught by Walker et al. Walker et al provides motivation by indicating that this method would ensure a more secure electronic commercial transaction by preventing the merchant or an intercepting third party from misusing the credit card information (Col. 3, lines 59-65).

Art Unit: 3621

As per **Claim 2**, Franklin et al further disclose wherein the corresponding transaction information provided by the merchant includes a name and/or address associated with the user (Col. 5, lines 29-32).

As per **Claim 3**, Franklin et al further disclose wherein the temporary authorization number includes an additional encrypted message authentication code generated from the multiple fields of information regarding the transaction using the secret information as a cryptographic key (Col. 5, lines 32-43).

As per **Claim 4**, Franklin et al fail to specifically disclose wherein the temporary authorization number includes a one-time encrypted password generated from information provided by the user and/or the credit card issuer, however, this would have been obvious to one having ordinary skill in the art. Franklin et al disclose that customer information is used to generate the encrypted MAC (such as customer's name, account number, etc.), however one skilled in the art would recognize that these are only examples and that any customer information may be used such as a customer password. The motivation would be to provide flexibility and provide more security by using different customer information to generate the MAC.

As per **Claims 5, 7 and 17**, Franklin et al disclose a method for facilitating credit card transactions over a telecommunications network based on authentication information provided by a user having an account with a credit card issuer, comprising the steps of:

- generating offline a temporary authorization number for the user based on secret encoding and encryption information shared with the credit card issuer (Col. 4, lines 55-65; Col. 5, lines 25-43);
- sending via the telecommunications network to an e-commerce merchant from the user the temporary authorization number containing the authentication information in a message authentication code utilized in a credit card transaction without disclosing a credit card account number via the telecommunication network to the merchant (Figure 1; Col. 5, lines 27-52);

Art Unit: 3621

obtaining via the telecommunications network a verification from the credit card issuer based on a comparison of a generated MAC and the MAC provided in the temporary authorization number using corresponding information regarding the transaction provided by the merchant (Col. 5 line 59-Col. 6 line 23).

Franklin discloses that the issuing institution uses the same cryptographic hashing function to compute a MAC and then compares the generated MAC with the MAC provided by the merchant, however, fails to disclose matching decoded fields of information with corresponding transaction information as recited in the claims. Walker et al disclose a method for generating a single-use financial account number by encrypting multiple fields of information such as an initialization variable, an a-bit account number and a nonce (Col. 7, lines 60-67; Col. 8, lines 8-36). Walker further discloses looking up secret information such as the cardholder's private key to decrypt the fields of information and compares this information to validate the transaction (Col. 8, lines 40-67). Walker et al further disclose that instead of encoding the account number as part of the credit card number, the name that appears on the card could take the place of the account number and further that more bits become available and can be used to encode a timestamp, purchase information or even merchant information (Col. 11, lines 8-19). Thus, it would have been obvious to one having ordinary skill in the art at the time of applicant's invention to modify the invention of Franklin and encrypt multiple fields of information by the user and then decrypt this information by the issuing institution and perform a comparison to validate the transaction as taught by Walker et al. Walker et al provides motivation by indicating that this method would ensure a more secure electronic commercial transaction by preventing the merchant or an intercepting third party from misusing the credit card information (Col. 3, lines 59-65).

As per **Claims 6 and 19-20**, Franklin et al further disclose wherein the multiple encoded fields of encrypted information includes as the authentication information a transaction amount, date information, account number and merchant ID (Col. 5, lines 25-35).

Art Unit: 3621

As per **Claim 8**, Franklin et al further disclose wherein the temporary authorization number includes an additional encrypted message authentication code generated from the multiple fields of information regarding the transaction using the secret information as a cryptographic key (Col. 5, lines 32-43).

As per **Claim 9**, Franklin et al fail to specifically disclose wherein the temporary authorization number includes a one-time encrypted password generated from information provided by the user and/or the credit card issuer, however, this would have been obvious to one having ordinary skill in the art. Franklin et al disclose that customer information is used to generate the encrypted MAC (such as customer's name, account number, etc.), however one skilled in the art would recognize that these are only examples and that any customer information may be used such as a customer password. The motivation would be to provide flexibility and provide more security by using different customer information to generate the MAC.

As per **Claims 10 and 18**, Franklin et al further disclose wherein the temporary authorization number has a format similar to a credit card number (Col. 5, lines 5-11 and 42-50).

As per **Claim 21**, Franklin et al further disclose wherein the corresponding transaction information provided by the merchant includes a name and/or address associated with the user (Col. 5, lines 29-32).

Conclusion

8. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the

Art Unit: 3621

THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

9. Examiner's Note: Examiner has cited particular columns and line numbers in the references as applied to the claims below for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as well. It is respectfully requested from the applicant, in preparing the responses, to fully consider the references in entirety as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior art or disclosed by the examiner.

10. The prior art previously made of record and not relied upon is considered pertinent to applicant's disclosure.

- Demoff et al disclose a system for providing temporary credit authorizations and teach a randomly generated credit transaction number and made valid only for the requested transaction
- Vizcaino discloses an apparatus for securing credit card transactions and teaches producing a verification number which is based on a transaction sequence number and an encryption algorithm stored in the device as well as a corresponding decryption algorithm stored in a verification computer. The verification computer matches a computed transaction sequence number to a stored transaction sequence number to verify the transaction.
- Stambler discloses securing information relevant to a transaction using a variable authentication number
- Flitcroft et al disclose a credit card system and teach providing limited use credit card numbers for single or limited use transactions

Art Unit: 3621

- Canfield discloses a method for verifying credit card transactions and teaches the use of a verification code number calculated by the customer and verified by the issuer
- Penzias discloses a system for fraud protection for credit card transactions and teaches that the customer may identify himself by supplying a card number.

Art Unit: 3621

11. Any inquiry concerning this communication or earlier communications from the examiner should be directed to John Hayes whose telephone number is (703)306-5447. The examiner can normally be reached Monday through Friday from 5:30 to 3:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jim Trammell, can be reached on (703) 305-9768.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 308-1113.

Please address mail to be delivered by the United States Postal Service (USPS) as follows:

**Mail Stop _____
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450**

Please address mail to be delivered by other delivery services (Federal Express (Fed Ex), UPS, DHL, Laser, Action, Purolator, etc.) as follows:

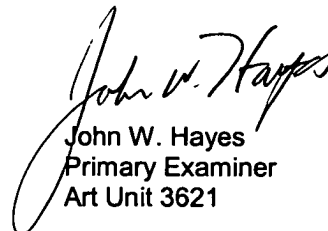
**U.S. Patent and Trademark Office
2011 South Clark Place
Customer Window, Mail Stop _____
Crystal Plaza Two, Lobby, Room 1B03
Arlington, Virginia 22202**

or faxed to:

(703) 872-9306 [Official communications; including
After Final communications labeled
"Box AF"]

(703) 746-5531 [Informal/Draft communications, labeled
"PROPOSED" or "DRAFT"]

Hand delivered responses should be brought to Crystal Park 5, 2451 Crystal Drive,
Arlington, VA, 7th floor receptionist.


John W. Hayes
Primary Examiner
Art Unit 3621

August 9, 2004